



Elsevier  
Harcourt Education  
LexisNexis  
Reed Business

January 19, 2007

*Via Electronic Filing (taskforcecomments@idtheft.gov)*

The Honorable Alberto R. Gonzalez  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530

The Honorable Deborah P. Majoras  
Chairman  
Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

Re: Comments to Federal Identity Theft Task Force

Dear Attorney General Gonzalez and Chairman Majoras:

Reed Elsevier Inc., on behalf of its LexisNexis division, appreciates the opportunity to submit comments in response to the Identity Theft Task Force's ("Task Force") invitation to comment on several issues regarding recommendations it will make in its final strategic plan to the President. We would like to commend the Task Force for the leadership shown on these important issues, and hope that our experience in this area will be useful as you develop your recommendations to help combat identity theft.

Reed Elsevier is one of the world's leading publishing and information companies, employing more than 20,000 people in the United States. LexisNexis is a leading provider of information-based products and services to a wide range of professionals in the legal, risk management, corporate, government, law enforcement, accounting and academic markets. LexisNexis' products and services help businesses and government manage risk through fraud detection and prevention, identity authentication, and intelligent risk scoring and modeling.

LexisNexis' identity authentication products help detect and prevent identity theft and fraud by allowing financial institutions, insurance companies, government agencies, and others to determine whether a person is who they say

they are. In addition, LexisNexis provides products and services that are used to help professionals locate people and assets, support national security initiatives, and facilitate background checks on prospective employees. LexisNexis staff includes subject matter experts in identity theft, identity management, and identity authentication.

LexisNexis is a founding partner of the Center for Identity Management and Information Protection ("the Center") at Utica College. The Center, under the leadership of Dr. Gary Gordon, is a research collaborative dedicated to furthering a national research agenda on identity management, information sharing, and data protection. The Center currently is conducting a study of Secret Service investigations into identity theft matters to determine who perpetrates identity theft and how, and effective means of investigation, the outcome of which will be used to help train law enforcement officers. This study is being funded by the Bureau of Justice Assistance.

Reed Elsevier and LexisNexis support the efforts of the Task Force to develop a coordinated strategy to combat identity theft. We hope that our input will assist the Task Force in developing recommendations on how to further enhance the effectiveness and efficiency of government activities to detect, prevent, and prosecute identity theft and fraud.

**Summary:**

We are pleased to provide the Task Force with our comments on a number of key topics. Our comments below are focused on the following five areas:

1. **Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information.** Consistent with the proposals outlined by FTC Chairman Majoras, we support establishing a single federal standard for security breach notification in the event of a security breach where there is a significant risk of identity theft to consumers.
2. **National Data Security Standards.** We support the establishment of a single federal standard for data security safeguards to protect sensitive personal information modeled after the Gramm-Leach-Bliley ("GLB") Act Safeguards Rule.
3. **Comprehensive Record on Private Sector Use of SSNs.** We believe that any recommendations regarding government or private sector use of Social Security numbers ("SSNs") should ensure that

legitimate businesses, government agencies, and other organizations continue to have access to identifying information that they depend on for important purposes including fraud detection and prevention, identity verification, locating missing children, identity theft prevention, law enforcement purposes, and other critical applications. Moreover, any recommendations should strike the right balance between protecting privacy and ensuring continued access to critically important information that businesses, government agencies, and other organizations need to do their jobs.

4. **Government Use of SSNs.** We support the Federal Trade Commission's ("Commission") efforts to hold workshops on and fully explore issues related to identity authentication. Moreover, we believe that any consideration of alternatives to SSNs as a unique identifier should be undertaken in the context of identity authentication to ensure that any concerns about misuse of SSNs or such alternatives in connection with identity authentication be explored.
5. **National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes.** We support a study to determine the feasibility of a national system for issuing identity documents to assist identity theft victims and to protect them from being mistaken for the suspect who has misused their identities. This study also should evaluate the feasibility of using information-based identity authentication to ensure that criminals do not use this system to the detriment of identity theft victims.

**Discussion:**

**1. Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information.**

We support establishing a single, federal standard for security breach notification in the event of a security breach where there is a significant risk of identity theft to consumers. Any federal data security breach law should include the following key elements:

- (a) a trigger for notification of consumers in instances where a security breach represents a significant risk of identity theft;
- (b) a definition of "sensitive information" that is limited to those data elements that are truly sensitive and can actually be used to commit identity theft;

(c) an exception from the definition of "sensitive information" for public record information; and

(d) federal preemption to ensure a uniform national standard to provide for consumer confidence and predictability for businesses.

Each of these elements is discussed briefly below.

### ***Trigger for notification***

Consistent with the remarks of Chairman Majoras in congressional testimony and other public forums, we believe that the "trigger" for breach notification should be limited to those breaches where there is a significant risk of identity theft. See, e.g., Remarks of Deborah Platt Majoras Chairman, Federal Trade Commission, at the Chamber of Commerce, Washington, DC, December 5, 2006, available at

<http://www.ftc.gov/speeches/majoras/061206chambercommerceremarks.pdf>.

This will go a long way toward preventing over-notification of consumers and ensuring that notice is meaningful. Indeed, this approach is consistent with the findings of leading studies on security breach issues, which have found that "strict automatic data breach notification laws 'regardless of risk' to the victim will saddle businesses with costly and unwarranted requirements, while providing little protective value to consumers." See, e.g., reports of Javelin Study and Research, including "Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses" ("Report"), August 2006, at page 1.

In addition, one significant risk to consumers directly resulting from security breach notifications is a marked increase in fraudulent phishing schemes. Consumers receive e-mails falsely attributed to a legitimate business that recently announced a security breach. The e-mail asks consumers to disclose account numbers and passwords in order to protect them from identity theft. These schemes in fact seek to cause consumers to disclose sensitive personal information in order to perpetrate fraud. We are concerned that over-notification could unnecessarily expose consumers to an increase in phishing schemes that could result in new instances of identity theft and fraud.

### ***Covered information***

It also will be important to ensure that the definition of "sensitive information" is limited to those data elements that are truly sensitive and can be used to commit identity theft.

Information such as credit card numbers and associated personal identification numbers ("PINs") should be protected. Generally available information, such as listed telephone numbers and street addresses, should not be protected, as this information is widely used by consumers and businesses, is not otherwise sensitive, and is not of the type used to commit identity theft.

### ***Public Record Exception***

The definition of "sensitive information" should explicitly exclude publicly available information, including information lawfully obtained from (1) Federal, State, or local government records; and (2) widely distributed media such as news reports, books, periodicals, directories, or sites on the World Wide Web. It makes no sense to require companies to impose additional security requirements on or notify consumers of security breaches of information that already is widely available and in the public domain. The vast majority of the states have included a public records exemption in their data security breach laws: to date, 31 of the 34 states that have enacted security breach notification legislation have included an exception for information obtained from public sources.

Moreover, this approach is consistent with the approach taken in section 501(b) of the GLB Act. This section has been interpreted to require notices to consumers where there has been unauthorized access to "customer information." Both the security breach notification guidance issued by the functional regulators, and the Safeguards Rule, exclude publicly available information from the definition of "customer information" and, thus, the safeguard and notice requirements.

### ***Federal Preemption***

Finally, it is critical that any national data security breach notification law contain federal preemption to ensure the application of a uniform national standard. The over 30 different state security breach notification laws referenced above all have varying requirements. It is essential that Congress pass federal legislation that would put in place a uniform national standard to protect consumers and promote consumer confidence, as well as to provide one set of rules for businesses to comply with.

## **2. National Data Security Standards.**

Reed Elsevier supports the adoption of data security requirements modeled after the GLB Safeguards Rule. Consistent with these requirements,

we believe that any regulations in this area should allow for flexibility and be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the consumer information it handles. In addition, such requirements should preempt state laws on this issue to ensure that companies not have to struggle with complying with multiple, potentially conflicting state laws.

### **3. Comprehensive Record on Private Sector Use of SSNs.**

Businesses, researchers, government agencies, and others rely on information contained in information solutions and services products, such as those offered by LexisNexis, to do their jobs. Companies like LexisNexis play a vital role by collecting information from numerous sources and creating comprehensive data collections that allow users to easily search and locate information.

In making any recommendations regarding both public and private sector use of SSNs, it will be important that the record reflect the critical role that SSNs play in detecting and preventing the fight against identity theft and fraud and in other socially beneficial uses.

The following are some examples of how SSNs contained in LexisNexis information solutions and services products are used to help people, protect consumers, and assist law enforcement efforts. The use of SSNs is critical for person identification and record matching purposes and is necessary to ensure the accuracy of the information.

SSNs allow persons to be identified accurately and ensure that records for different individuals do not get co-mingled. For example, there are tens of thousands of individuals named Robert Jones in the U.S. How can one individual be distinguished from another? A unique identifying number like the SSN is important to ensure that information about an individual is accurately associated with that individual.

SSNs also are used by companies to help combat identity theft and fraud. In fact, such information utilized in customer acquisition solutions prevents a continued rapid increase of identity fraud victims. SSNs are a critical tool used for a variety of beneficial purposes including:

- **Locating sex offenders**—SSNs are used to locate registered and unregistered sex offenders. There are over 560,000 sex offenders in the U.S. Approximately twenty-four percent of these individuals fail to comply with address registration requirements mandated by law.

Access to SSNs allows law enforcement to locate sex offenders even when the registration address has not been kept current.

- **Law enforcement**—SSNs are used routinely by public and private law enforcement officials to locate fugitives and witnesses to crimes. The ability to conduct an information search using an SSN is essential. Restrictions on access to SSNs in government records would hamper our ability to provide this critical information to our law enforcement clients.
- **Locating and recovering missing children**—LexisNexis has partnered with the National Center for Missing and Exploited Children to help that organization locate missing and abducted children. Locating a missing child within the first 48 hours is critical. After that time, the chance of recovering the child drops dramatically. In many of these cases, it is the non-custodial parent who has taken the child. The use of SSNs is critical in locating the non-custodial parent and recovering the missing child. This effort will be seriously hampered if SSNs in public records are no longer available.
- **Child support recovery**—Public and private agencies rely on social security numbers and other information contained in information solutions and services products to locate parents who are delinquent in child support payments and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for Enforcement of Support (ACES), a private child support recovery organization, has stated that social security numbers are the most important tool for locating parents who have failed to pay child support. ACES has had tremendous success using LexisNexis to locate nonpaying parents using LexisNexis products.
- **Credit card fraud prevention**—Public record information compiled using SSNs is routinely used to detect fraudulent credit card applications. This identifying information is used to prevent identity theft and fraud by allowing companies to prescreen applications to ensure that the address, phone number and other information of the applicant matches the applicant's name.
- **Insurance fraud prevention**—Insurance companies use public record information compiled using social SSNs to detect fraudulent insurance claims. According to the National Fraud Center, the average American household pays \$200 to \$400 a year in additional insurance premiums to offset the cost of fraud. This cost would likely increase if companies

do not have the information they need to detect and prevent fraud.

- ***Preventing and investigating financial crime***—LexisNexis is the preferred provider of public records at the Financial Crimes Enforcement Network (FinCEN) under the U.S. Treasury Department. FinCEN supports federal, state and local law enforcement agencies in financial investigations and is heavily reliant on SSNs in these investigations. In addition, LexisNexis is working on a project with the American Bankers Association to develop best practices to be used by banks and other financial institutions to prevent money laundering and ensure compliance with the USA PATRIOT Act. The use of SSNs by financial institutions to verify and validate information on prospective customers will be critical to the success of that program.
- **Location of missing heirs**—SSNs are an important tool used in locating pension fund beneficiaries and missing heirs to ensure they receive the money owed them. Pension Benefit Information (PBI), a private company that locates former employees that are due pension benefits, has indicated that in many cases the SSN becomes the only link between an employer and their former employees with vested benefits. Employees move, marry and change their name, but the one thing that remains constant is their SSN.

#### **4. Government Use of SSNs.**

It is generally accepted that maintaining the accuracy of information in government files is critical to the efficient operation of the government. This need for accuracy will make it difficult for government to discontinue the use of SSNs as a unique identifier. Rather than abandoning use of SSNs or creating an alternative identifier to be used in lieu of SSNs, the government should look to reduce instances of unnecessary use and take steps to protect SSNs from unauthorized disclosure where use is necessary. The government should also guard against use of SSNs as an authenticator, as such misuse is what imparts value to SSNs and creates the risk of misuse.

Because the SSN is the only identifier uniquely and permanently assigned to U.S. residents, it is an essential component of identity authentication and fraud prevention tools. As noted above, it is important to preserve access to and use of SSNs from a variety of sources for legitimate business and law enforcement purposes to help ensure the effectiveness of fraud prevention and identity verification tools, and limit unnecessary exposure of businesses and consumers to potential harm.

The true value of an SSN is as a unique identifier and the ability to use an SSN to aid in matching information across records and systems. The Task Force should be mindful that the danger of using an SSN lies not in using it as an identifier, but rather in widespread misuse of SSNs as authenticators. Possession of an SSN should not be used as evidence of identity.

Moreover, if a new identification number is created and substituted for SSNs, as referenced in section I.1 of the Task Force's request for comments, many of the same concerns that currently surround use of SSNs will quickly be replicated. Some organizations will begin to use the new identification number as proof of identity, thus adding value to mere possession of this number. Use of the number as proof of identity--as an authenticator--will result in new risks of identity theft or fraud for consumers through possession of the new number.

#### **5. National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes.**

There is significant anecdotal evidence that a consumer can experience difficulties with the criminal justice system after becoming a victim of identity theft. Actions of the thief can be wrongfully attributed to the victim. Victims can have difficulty establishing their innocence. We support a study to determine the feasibility of a national system for issuing identity documents to assist identity theft victims and to protect them from being mistaken for the suspect who has misused their identities.

For an alternative identity document or "passport" to work, it is critical that the identity of the individual be authenticated prior to issuance. Unless the individual is authenticated, identity thieves could use this system to perpetuate their crime, to the further detriment of the victim. This study should evaluate the feasibility of using information-based identity authentication to positively identify participating individuals and to ensure that criminals cannot use this system to the detriment of identity theft victims.

\* \* \*

In conclusion, Reed Elsevier and LexisNexis support the Task Force's goal to develop a coordinated strategy to combat identity theft, including efforts to educate consumers on ways to protect themselves from identity theft and fraud and assisting victims of ID theft in recovering from this crime. We also strongly support government efforts to aggressively prosecute those who commit identity theft and related crimes.

We appreciate the opportunity to submit comments on these important issues. We hope that our comments will help the Task Force in developing recommendations on how to further enhance the effectiveness and efficiency of government activities to detect, prevent and prosecute identity theft and fraud. If you have any questions regarding our comments, please call me at 202/857-8253 or contact Steve Emmert of my staff at 202/857-8254.

Steven M. Manzo  
Vice President, Government Affairs  
Reed Elsevier Inc.